Vertiv CYBEX™ SCUSBACFILTER

Firmware Version 40404-0E7

Common Criteria Guidance Supplement

Doc No. 2149-001-D105C4B
Version: 1.8
19 January 2022

Vertiv
1050 Dearborn Dr,
Columbus, OH 43085

Prepared by:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J 7T2

CONTENTS

LIST OF TABLES

1 PREPARATION OF THE OPERATIONAL ENVIRONMENT

1.1 OPERATIONAL ENVIRONMENT

For secure operation, users are required to ensure the following conditions are met in the operational environment:

- TEMPEST approved equipment may not be used with the secure peripheral sharing device
- The operational environment must provide physical security, commensurate with the value of the peripheral sharing device and the data that transits it
- Wireless keyboards, mice, audio, user authentication, or video devices may not be used with the secure peripheral sharing device
- Peripheral sharing device Administrators and users are trusted individuals who are appropriately trained
- Administrators configuring the peripheral sharing device and its operational environment follow the applicable security configuration guidance
- The HID filter is built to be locked in the USB port. The units for testing are not locking as they are not able to be released. This is not a tested functionality and is not critical. This is not critical for the operation for the TSF.

2 SECURE ACCEPTANCE PROCEDURES

Vertiv peripheral sharing devices may be purchased directly from Vertiv, or through distributors and resellers / integrators.

Upon receipt of the Vertiv peripheral sharing device, the customer can verify the configuration and revision by comparing the part number and revision on the packing list with the label on the bottom of the hardware unit. The nameplate includes the product part number (CGA) which is linked directly to the revision of the hardware components and firmware. Verification of the part number provides assurance that the correct product has been received.

The customer must download product documentation from the Vertiv website in Adobe Acrobat Portable Document Format (PDF). The customer can confirm that the documentation matches the purchased model.

Customers are instructed to check all delivered products for package container seals, and to verify that product tampering evident labels are intact. If an issue is discovered, the customer is instructed to return the product immediately.

3 SECURE INSTALLATION PROCEDURES

This section describes the steps necessary for secure installation and configuration.

3.1 SECURE INSTALLATION

Instructions for secure installation may be found in the Quick Installation Guide.

4 SECURE OPERATION

This section describes the steps necessary for the secure operation of the Vertiv USB HID Filter.

4.1 SELF TESTS

A self test is performed at power up. Self test failures may be caused by an unexpected input at power up, or by a failure in the device integrity. A self test failure may also be an indication that the device has been tampered with.

A user may enter self test failure mode by following the procedures outlined in Table 1.

Device Type	Procedure
HID Filter	1. To enter self test failure mode, connect an illegal device. The USB port is disabled and the LED flashes. 2. To exit self test failure mode, cycle the power by reconnecting to the computer.

Table 1 – Procedure to Initiate a Self Test

In the case of a self test failure, users are directed to contact Vertiv Technical Support.

4.2 ERROR STATE

As the product powers up, it performs a self-test procedure. Following failure of a self-test, the device will enter an error state. The error state is indicated by flashing of the Light Emitting Diode. At this point, the device will be inoperable. It will not accept input from any peripheral device.

The user can cause the self-test to be rerun by unplugging the device and plugging it back in.

4.3 TAMPER EVIDENT LABEL

The device is fitted with a holographic Tampering Evident Label placed at a critical location on the device enclosure. If the label is removed, the word 'VOID' appears on both the label and the product surface. If the tamper evident label is not intact, users are directed to discontinue use of the device and to contact Technical Support.